AFRL-RX-TY-TP-2009-4531

AUTOMATED RISK ANALYSIS TOOL TO SUPPORT TRANSFORMATION OF US AIR FORCE SECURITY FORCES (BRIEFING SLIDES)

Kenneth Knox

Applied Research Associates
P.O. Box 40128
Tyndall AFB, FL 32403

JUNE 2009

Presented at the Security Analysis and Risk Management Association (SARMA) Conference, 16-18 June 2009, held at the George Mason University in Arlington, Virginia.

AIRBASE TECHNOLOGIES DIVISION
MATERIALS AND MANUFACTURING DIRECTORATE
AIR FORCE RESEARCH LABORATORY
AIR FORCE MATERIEL COMMAND
139 BARNES DRIVE, SUITE 2
TYNDALL AIR FORCE BASE, FL 32403-5323

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
16-JUN-2009	Conference Presentation POSTPRINT	27-MAR-2007 -- 27-MAY-2009

4. TITLE AND SUBTITLE

Automated Risk Analysis Tool to Support Transformation of US Air Force Security Forces (BRIEFING SLIDES)

5a. CONTRACT NUMBER

FA4819-07-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

99999F

6. AUTHOR(S)

Knox, Kenneth

5d. PROJECT NUMBER

GOVT

5e. TASK NUMBER

F0

5f. WORK UNIT NUMBER

Q240FB6G

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Applied Research Associates
P.O. Box 40128
Tyndall Air Force Base, FL 32403

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory
Materials and Manufacturing Directorate
Airbase Technologies Division
139 Barnes Drive, Suite 2
Tyndall Air Force Base, FL 32403-5323

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RXQF

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

AFRL-RX-TY-TP-2009-4531

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

Ref AFRL/RXQ Public Affairs Case # 09-080. Presented at the Security Analysis and Risk Management Association (SARMA) Conference, 16-18 June 2009, held at the George Mason University in Arlington, VA. Document contains color images.

14. ABSTRACT

The Automated Risk Analysis Tool to Support Transformation of US Air Force Security Forces briefing provides an overview of AFRL's risk analysis methodology and the software tool ForcePRO. Discussed is the research from AFRL, Airbase Technologies Division, Integrated Defense Technologies vulnerability and risk assessment support to the Air Force's Security Forces Center.

15. SUBJECT TERMS

risk analysis, security forces, ForcePRO, integrated defense, risk management, risk factors, risk tolerance, assessment tools, vulnerability, asset rating, threat assessment, Defense Threat Assessment (DTA), vulnerability assessment

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Walt Waltz
U	U	U	UU	41	19b. TELEPHONE NUMBER *(Include area code)*

Reset

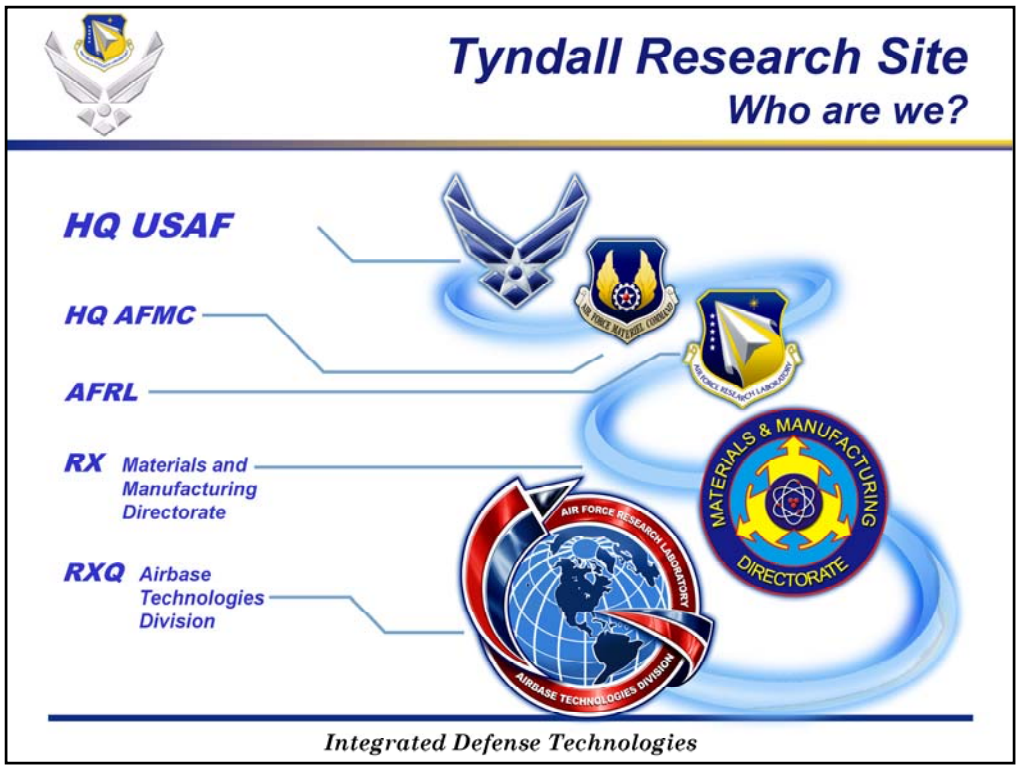
Automated Risk Analysis Tool
to Support Transformation of US Air Force Security Forces

AFRL
THE AIR FORCE RESEARCH LABORATORY
LEAD | DISCOVER | DEVELOP | DELIVER

Dr Ken Knox
Integrated Defense Technologies
Airbase Technologies Division
Tyndall AFB FL

- Introduce self

- We'll briefly cover our organization
- Why are the Security Forces (SF) in need of transformation
- History of AFRL's involvement with security risk analysis
- Introduce the risk analysis methodology and the software tool ForcePRO



I am a support contractor to the Air Force Research Laboratory, Airbase Technologies Division at Tyndall. The Airbase Technologies Division is the AF's only Agile Combat Support (ACS) research and development organization. As the name suggest, we support ACS career fields in finding solutions to the challenges of conducting lighter, leaner, and more efficient airbase operations.

We have been providing vulnerability and risk assessment support to the Air Force Security Forces Center since 1999.

Requirement for SF Transformation

- Why Change – Why Now?
  - SF career field challenges
    - Manpower
    - Deployments
    - Funding

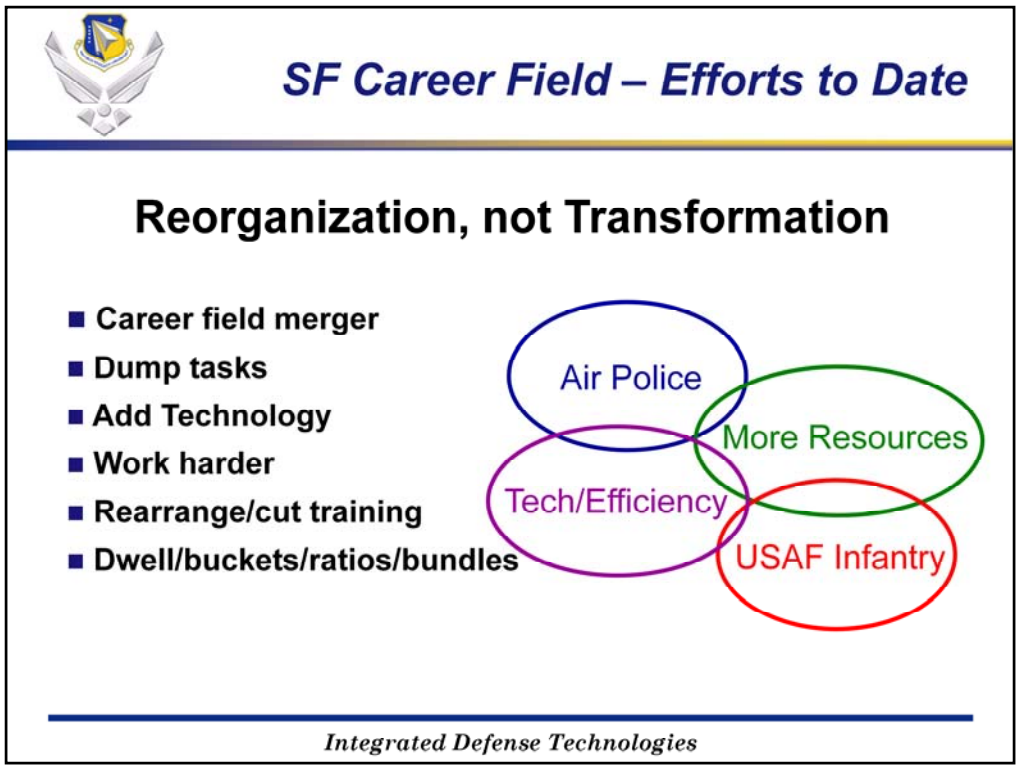
Integrated Defense Technologies

Why do need a new process for determining defense requirements for an installation? And why do we need it now?

The answers can be found by looking at the challenges facing the security forces today.

We do not have the manpower to meet all our home stations requirements to start with,

Add the deployment requirements and the shortages in funding for technology and technology sustainment and we all can see we can't get there from here.



We've made several attempts as a career field to transform ourselves, but for the most part we've reorganized instead of transforming.

We merged our career field into one AFSC

We dumped some of our traditional tasks, but kept other tasks unsure if they added value or not

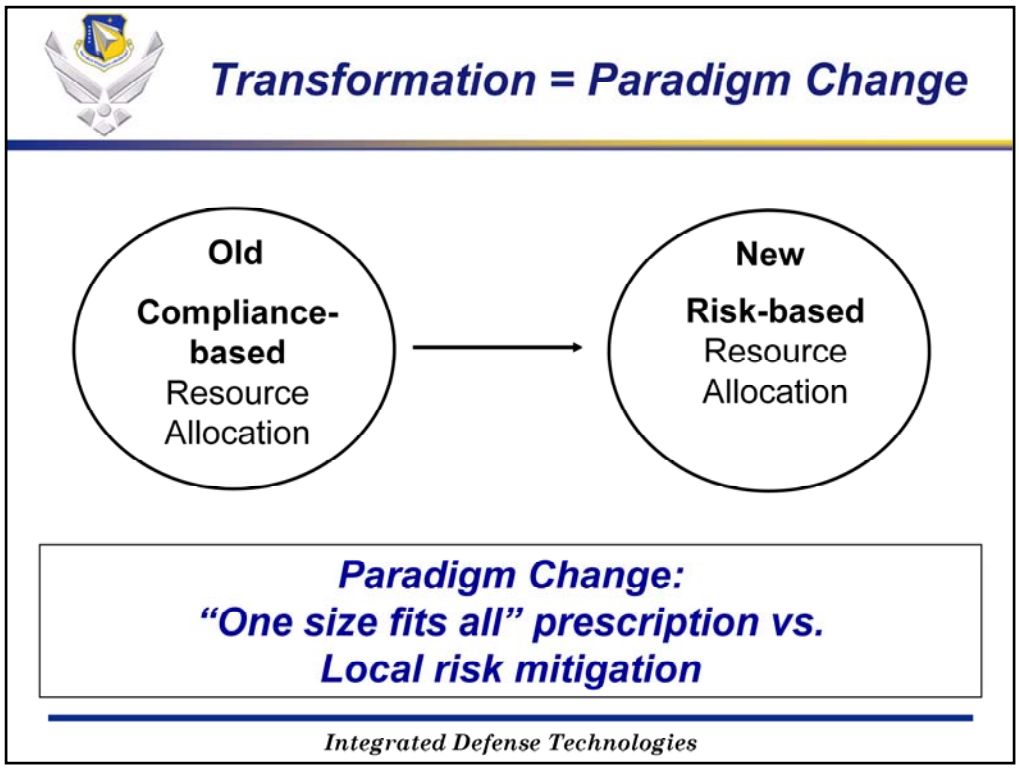
We've added technology, most of the time adding a sustainment burden to support the new equipment

We've adjusted flight schedules and shifts to try to cover all our requirements

We've rearranged or cut much needed training

And have met deployment taskings by increasing dwell, adding buckets, creating ratios and even bundling our folks for increased capability.

We've gone through all these changes but for the most part have kept to the basic standards we've had for the last 60 years in determining security on our installations.



In order to meet all the challenges of the modern era we need a new approach in determining defense requirements for an installation.

Former policy was compliance-based, presumed composite security data and mandated generalized protection measures; i.e., the "corporate" solution: "one size fits all."

Former policy produced inefficient utilization of security resources.

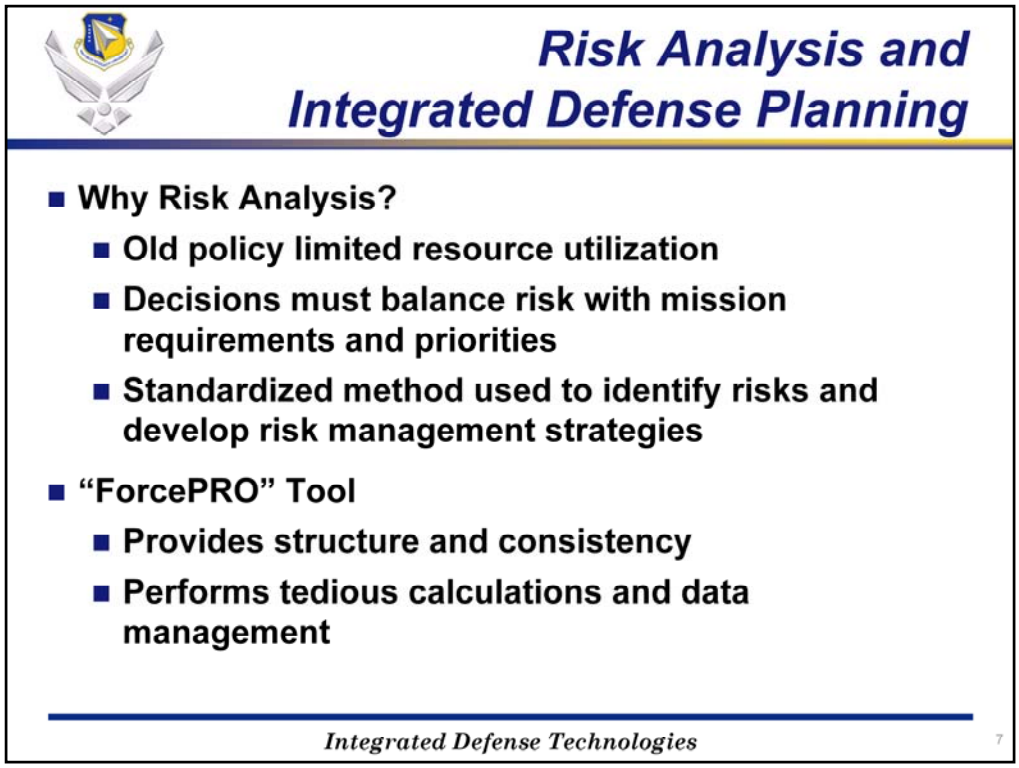
New policy is effects-based, uses analysis of real-time local intelligence data and specific security conditions, and provides situational awareness on which to base risk mitigation decisions; i.e., the field commander solution: locally-tailored security measures.

New policy enables maximum value of security resources.

Risk-based decision making is a truly revolutionary approach to determining how we conduct our business

It strips away the old standards-based security practices that were risk averse, relied on directive orders to tell a defense force who, what and how to protect an installation and focused on the protection of PL level resources.

Today we've come to realize we can't protect everything, and everybody, from every threat. We are simply too resource constrained to pursue that lofty goal. We need an approach acknowledging some risks are acceptable, giving the defense force



• Why risk based security? We do not have the resources (funds, materials, and manpower) to protect every asset on every installation.

• We can strike a balance with risk and mission accomplishment by analyzing

- What assets are truly critical to the installation?
- What threat actors are in my area of concern to the installation?
- How the threat actors hurt the installation?

• A good risk analysis answers the "so what" of any vulnerability.

• Risk analysis will allow SF to transition from typical standards-based security practices to effects-based activities mitigating risk to the installation.

- Provides the means to develop effective polices, procedures and investment decisions.

• To assist in the risk analysis process, AFRL developed a software tool to implement the ForcePRO methodology of risk analysis after vetting the methodology by conducting assessments in USAFE and AMC. ForcePRO was developed to relieve the analyst of the burden of making a large number of hand calculations

• Overarching purpose of a risk analysis is a standardized process to organize data so decision makers can make informed decisions about risk.

  • The analysis process organizes existing information, applies standardized scales, and helps make a coherent, compelling argument for necessary changes to buy down unacceptable risk

• Following a standard process of analysis also enables measurement of the benefits of various countermeasure courses of action, ensuring they are effective in achieving true risk reduction

Challenges to New Risk Model

- Embracing a new way of doing business
- Facilitates analysis – not a "black box" process
- Requires:
  - Thought – analysts must use judgment (experience), not just follow prescription
  - Integrity – multiple analysts (eyes), mitigate bias and agendas
- We often lack the information we want or need
  - Limited data on threats
  - Some costs are hard to quantify (human life, political impact)
  - Risk factors can change rapidly

Integrated Defense Technologies

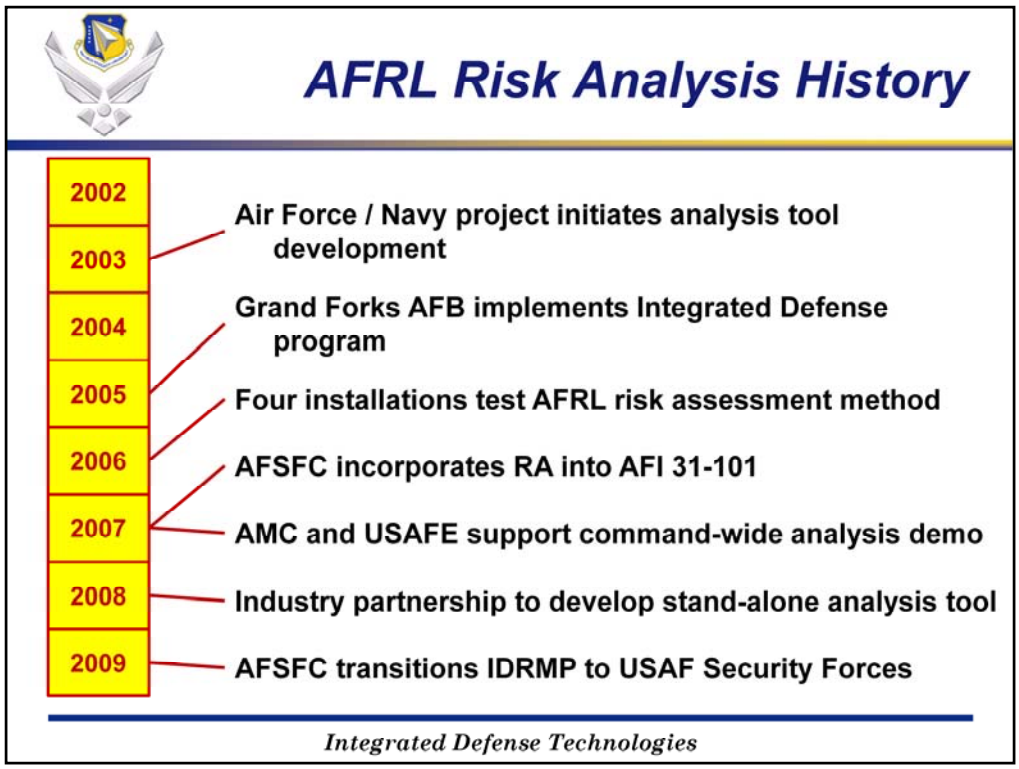
As with any new process there are challenges with its implementation. There are always those who resist change no matter if its easy or hard…its just change. It is a leap of faith for us to trust in our ability to deviate from the standards based security because we've always "done it that way"

This is not a black box process. It's not a piece of software that you type in a bunch of information and it spits the solution out the other side. This process requires: Thought…the analyst must use reasoned judgment when entering data into the process. Everything from deciding what an asset is, to how "bad" are the threat actors, to how effective are existing countermeasures and any proposed courses of action. The entire process requires engaged efforts to produce a quality product.

And you have got to work exceptionally hard to eliminate your bias and check agendas at the door when engaged in the process. If you have a certain bias for an asset, threat, countermeasure, etc. then you run the risk of under or overstating the element itself. If you have an agenda…"justify expense of new barriers system", or you measure the success of your defense program by the number of awards won or the amount of funding captured each year you may have a bad product at the end of the day. Honesty through the process is paramount

You'll never sit down with all the info you need the 1st time. You'll have to work hard to get it right.

- One of the biggest challenges we face in conducting a risk analysis is the lack of information available on threat actors in our areas of responsibility.
- We have lots of vulnerability assessments (including JSIVA, Food, Water, Base Security Zone and CIP assessments, SAVs, Program reviews and Inspections) pointing out our flaws and problems, but very little to tell us if we care, if the shortfalls really matter.
- Costs (and benefits) can be hard to measure (especially human life), although the new methodology should make this more quantifiable and easier, if not less controversial.
- Often risk factors (notably threats) can change, and frequently … ForcePRO should make keeping up with changes easier.



• ForcePRO was initiated in 2002 as a Joint Navy/AF project to develop decision support tool to assist Installation AT Officers in performing an installation risk analysis as prescribed by DoD Handbook 2000.12-H. Funding was lost to complete the project beyond prototype, however methodology development continued through a few grass roots efforts at a few initial sites.

- Using this prototype and a subsequent Microsoft Access tool with more flexibility, AFRL conducted RAs at numerous locations as part of its research into risk analysis
- AMC and later USAFE were aware of the RA efforts, and adopted “effects based security” as the command standard. They commissioned the lab to conduct MAJCOM-wide RAs using standardized approaches that would permit comparing the risks at one base with another … a first
- During this same time period, USAF security forces turned to a risk-based approach to their operations in order to address chronic shortages of people and equipment. AFRL contributed their RA methodologies to the new Integrated Defense instruction, AFI 31-101, and developed an updated version of ForcePRO for roll-out with the new AFI. The ForcePRO risk methodology is the cornerstone of the Integrated Defense Risk Management Process (IDRMP).

CONUS Risk Assessments

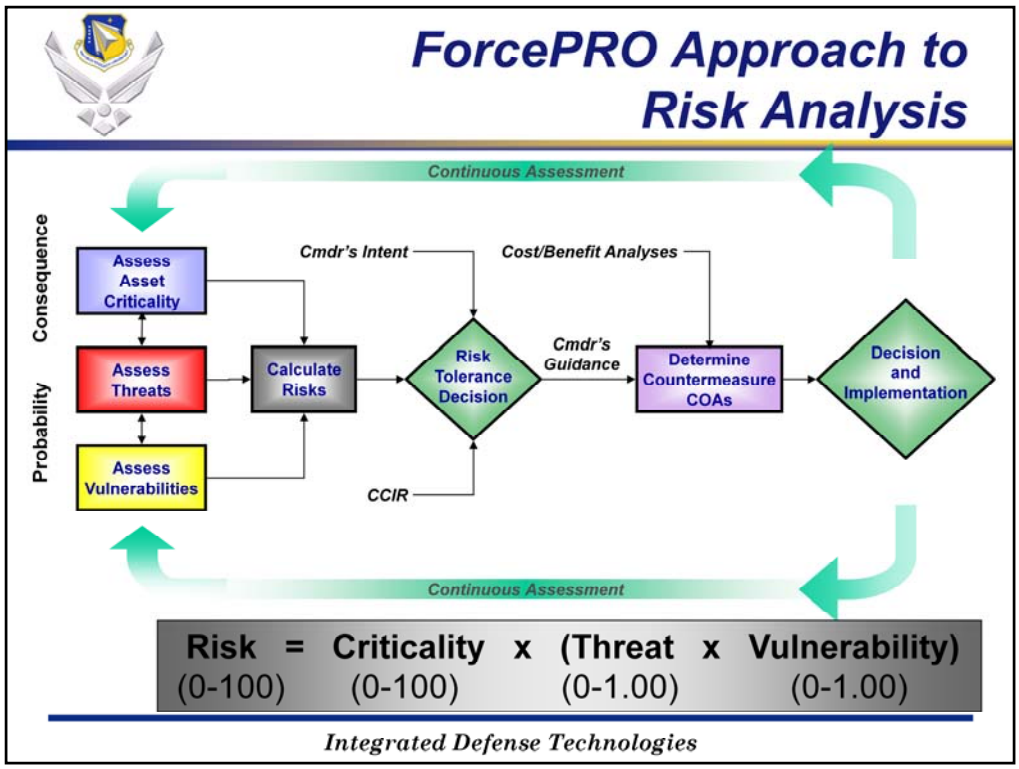
Key Points:

• These are the locations in CONUS that have received AFRL risk analyses.

USAFE Risk Assessments

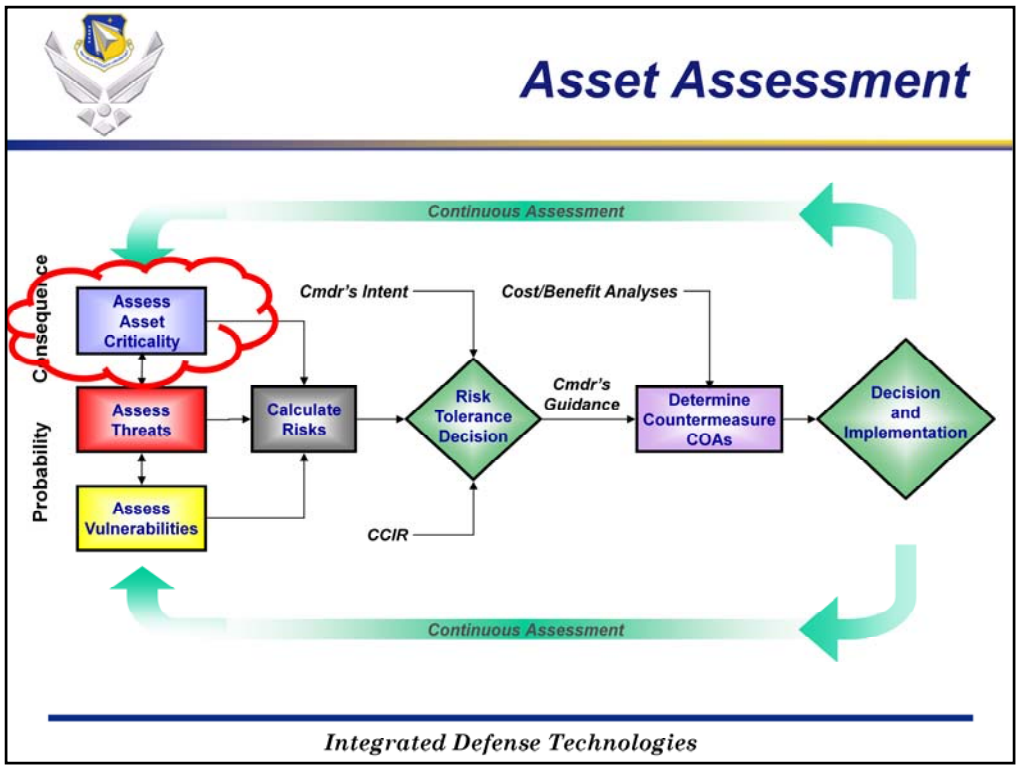
Key Points:

- 16 sites in USAFE also received risk analyses



Key Points:

- The risk analysis model has seven steps:
  - Risk Assessment
    - You have something you value – Assess Asset Criticality.
    - There are things that can hurt what you value – Assess Threat.
    - How can what you value be hurt – Assess Vulnerability.
    - By assigning values to Asset, Threat and Vulnerability and multiplying them in the formula below, we can calculate risk.
  - Risk Tolerance Decision – what can the commander "live" with?
  - Courses of Action Development – for the unacceptable risks, what mitigation Courses of Action are available, and at what cost and benefit?
  - Decision and Implementation – risk analysis by itself is not the goal. We want to use this tool to truly, and measurably, improve our security posture.



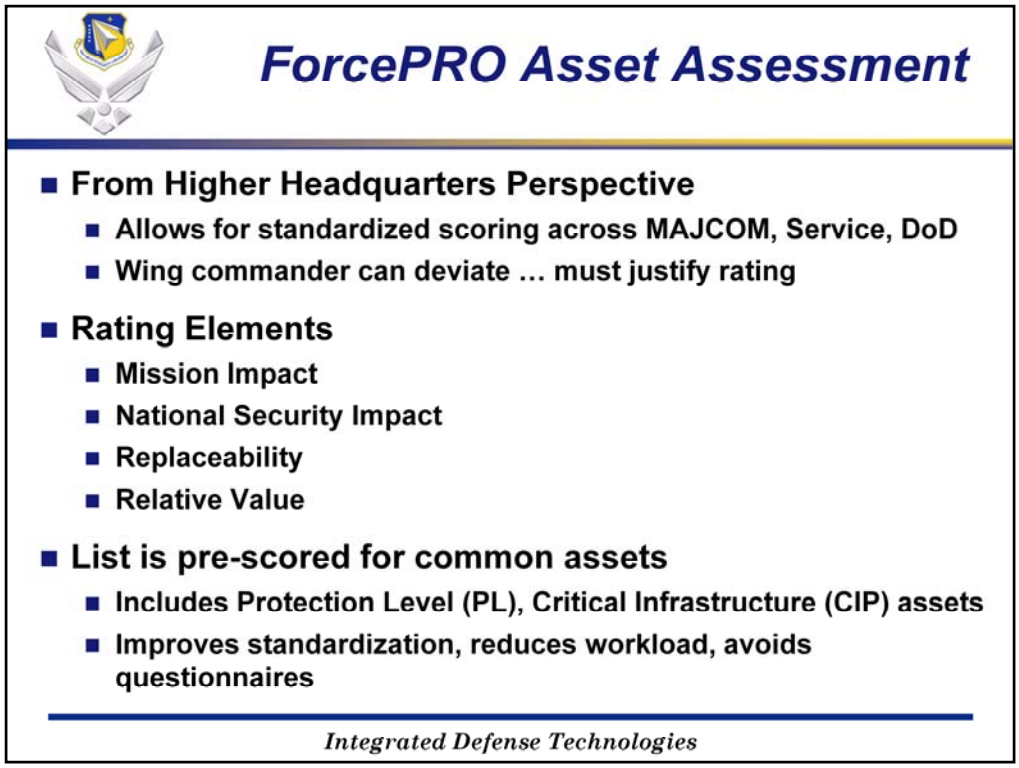
• We discussed the process in general terms and now let's break down the individual steps.

• Step 1 Asset Assessment is designed to answer the following questions:

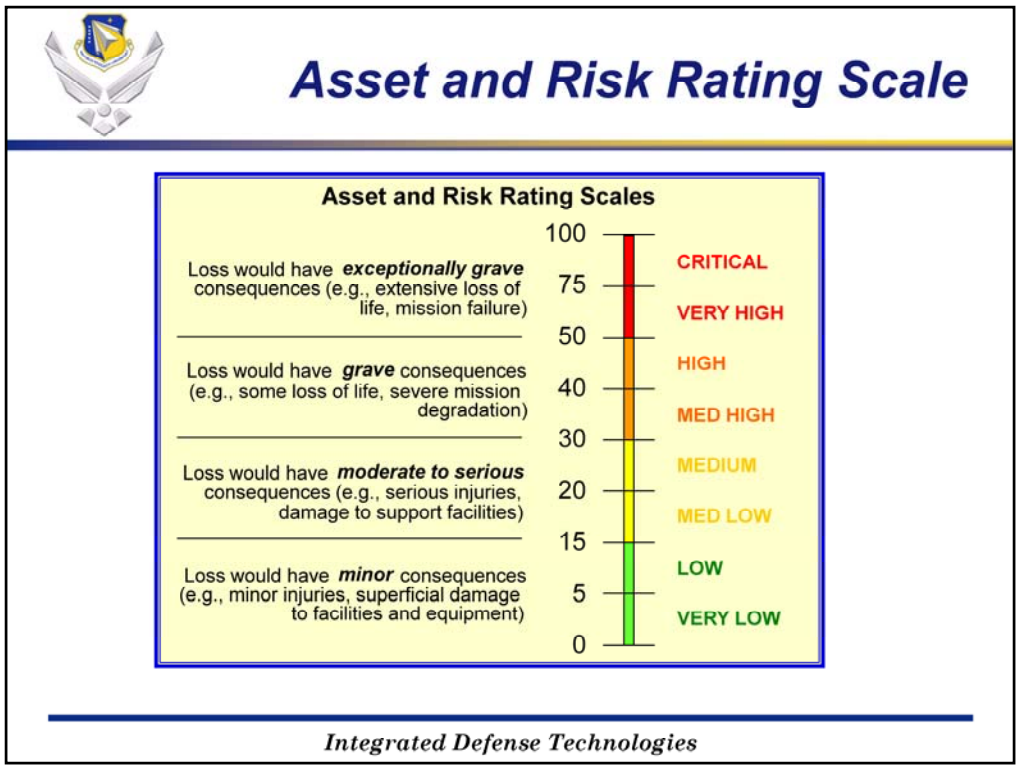
  • What have we got to protect?

  • Which assets are most important?

  • And finally, What would be the consequences if an asset were destroyed or obtained by your adversaries? Asset criticality *measures* the consequence of loss.

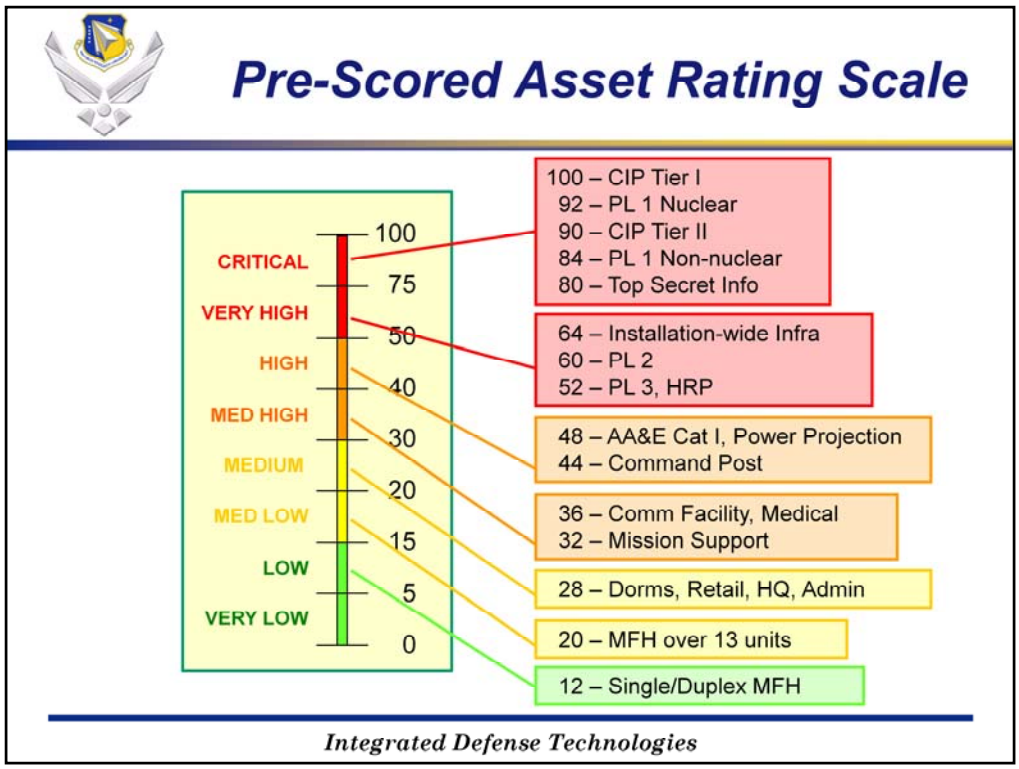


- The ForcePRO model views asset value from a higher headquarters perspective.
    - The allows for a level playing field when scoring assets across a command, service or even the DoD. A commander can deviate but must justify why.
- ForcePRO rates assets against four factors
    - Mission – how important is the asset to the installation mission?
    - National Security – how important is the asset to a higher headquarters?
    - Replaceability **of function** – how easily and quickly can the asset's function be replaced? For example, dining hall might take two years to replace if destroyed, but the function (feeding people) is immediately replaced
    - Relative Value – describes the value of the asset based on the type of asset, and allows us to compare apples and oranges. Depends on the category:
        - For buildings, usually based on number of people
        - For aircraft, is it a trainer or a strategic bomber?
- The first three factors are weighted equally, whereas the relative value is double-weighted
- The scores range from 0 to 100
- We use pre-scored assets to help standardize the scoring process
    - There are 39 categories of pre-scored assets, such as aircraft, mission support facilities, etc
    - The pre-scores establish the starting point, and unique aspects of the assets can then adjust the score so that the asset rating reflects its value to the installation



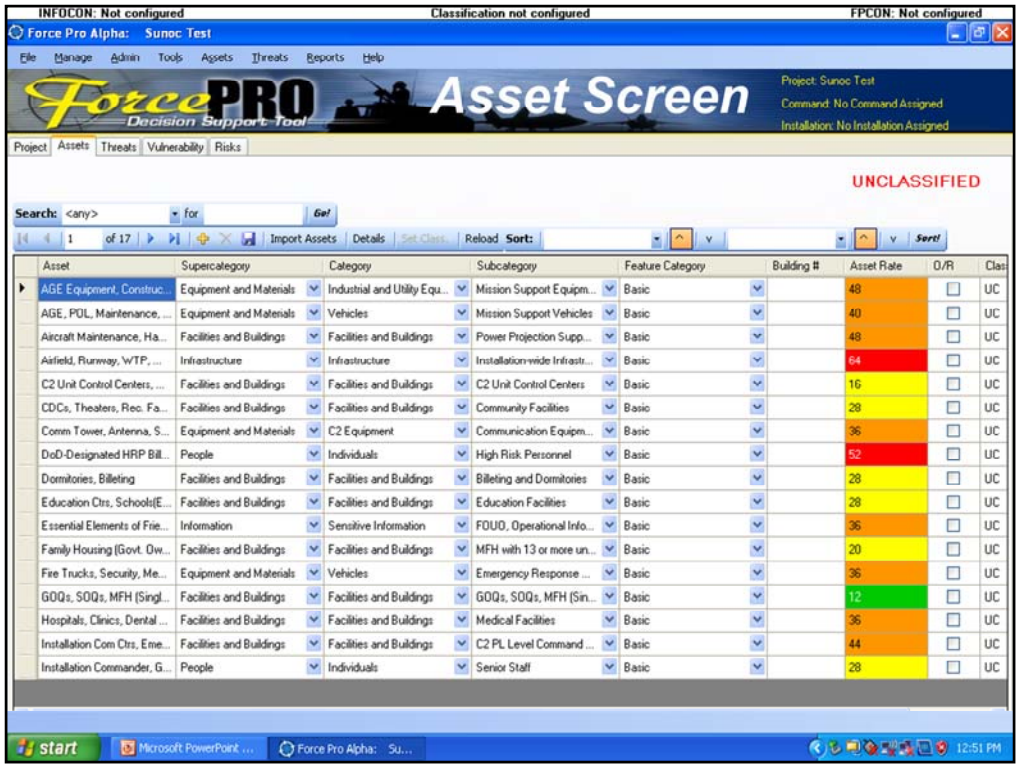
• All risk factors are tied to a scale that combines description, numbers, colors and adjectives. The asset and risk scales are identical – since asset rating measures the value of an asset to the installation, loss of that asset cannot exceed its value.

  • For assets that don't exactly fit the drop down factors to score, you should be familiar with this scale in order to override scores and place them in the correct place on the scale

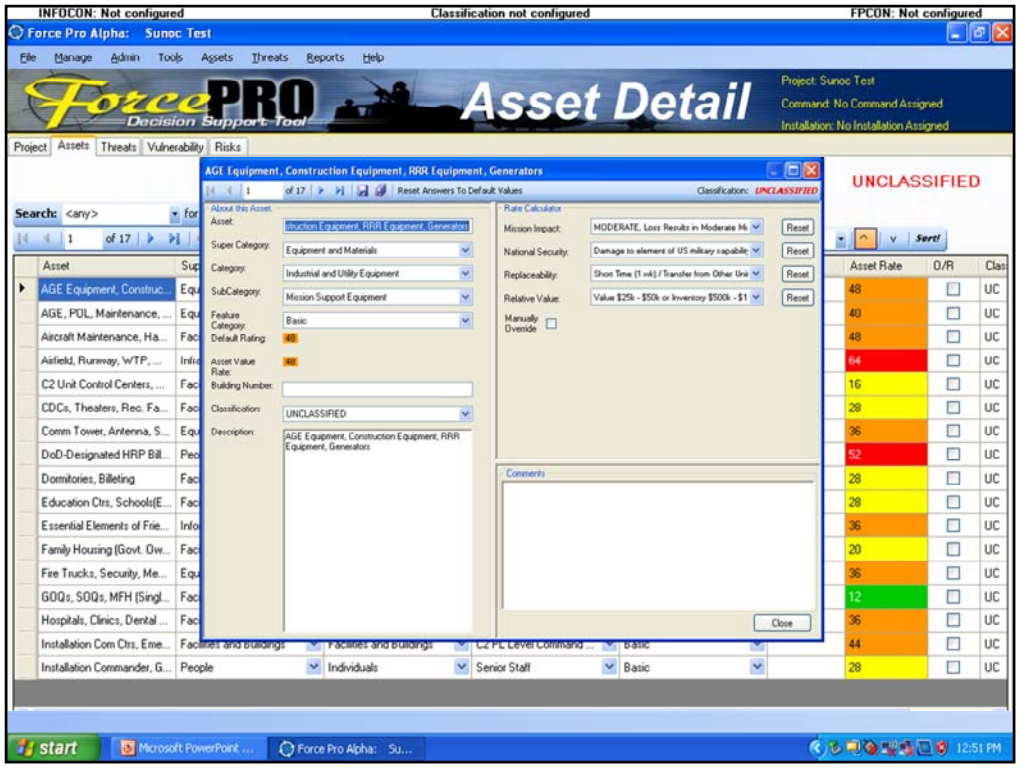


• Pre-scored assets shown, actuals vary based on Mission, National Defense, Replaceability, Relative Value (e.g., population)

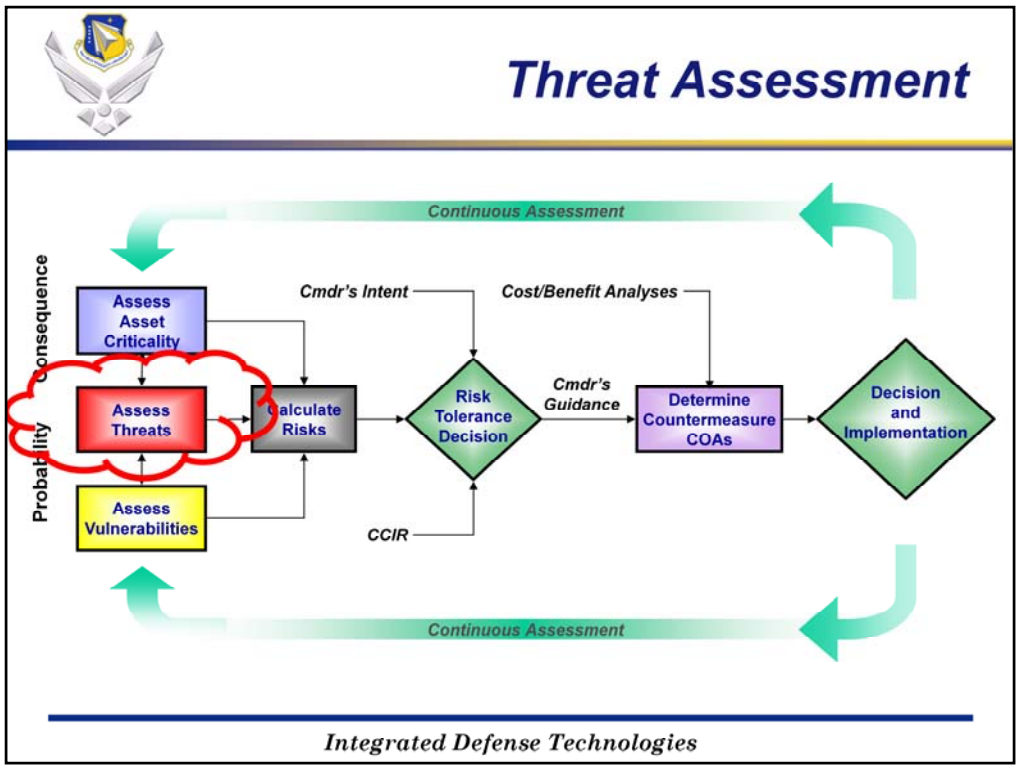
• Typically, critical mission assets are on top, mission/population centers in the middle, and general population centers near the bottom



- Screen capture from ForcePRO
  - Asset is **your** name for the asset
  - Supercategory/category is how ForcePRO manages data – the tactics and countermeasures for various categories (buildings, equipment, people) are different
  - Feature – most installation assets will fall under “Basic”, but some might be close to a perimeter, or are off-base, and their vulnerability ratings will be different. The feature makes scoring vulnerabilities MUCH easier.
  - Asset Rating – the score (0-100) for the asset.



• This detail screen allows you to completely customize the asset scoring, including overriding the default data (must justify), and adding comments and description



• The next major step in the RA is the threat assessment. When assessing the threat, we are really asking "who are we protecting the base from?" Adversaries can range from petty thieves focused on stealing audiovisual equipment to terrorist organizations capable of employing weapons of mass destruction.

• As we look at threat we need to ask and sufficiently answer three questions.

- Who is in our AOR? Terrorist, FISS, Criminal, etc.
- What tactics do they use and what targets are they after? FISS uses solicitation and eavesdropping to target information while terrorist use explosives to go after people.
- When assessing adversaries we need to understand their intent, capability and history of attacking assets to accurately determining their threat rating.

• The ForcePRO methodology uses existing info (DTA), along with working with threat specialists (AFOSI, wing Intel, SF, ATO, TWG, local PD, FBI, etc) to describe the **local** threat picture

• As called for in the Antiterrorism Handbook, we examine and score four major factors resulting in score from 0 to 1.00 for each adversary:

- Activity – what are the adversaries doing in the local area? (fundraising or targeting US)
- Sentiment – what is the history, philosophy, intent of the adversary? (Anti-US, attacks overseas)
- Capability – what do they like to do in the local area? (explosives, MASCAL, theft?)
- Environment – does the adversary operate with the same freedom of movement as we do? (favors adversary, US, neutral)

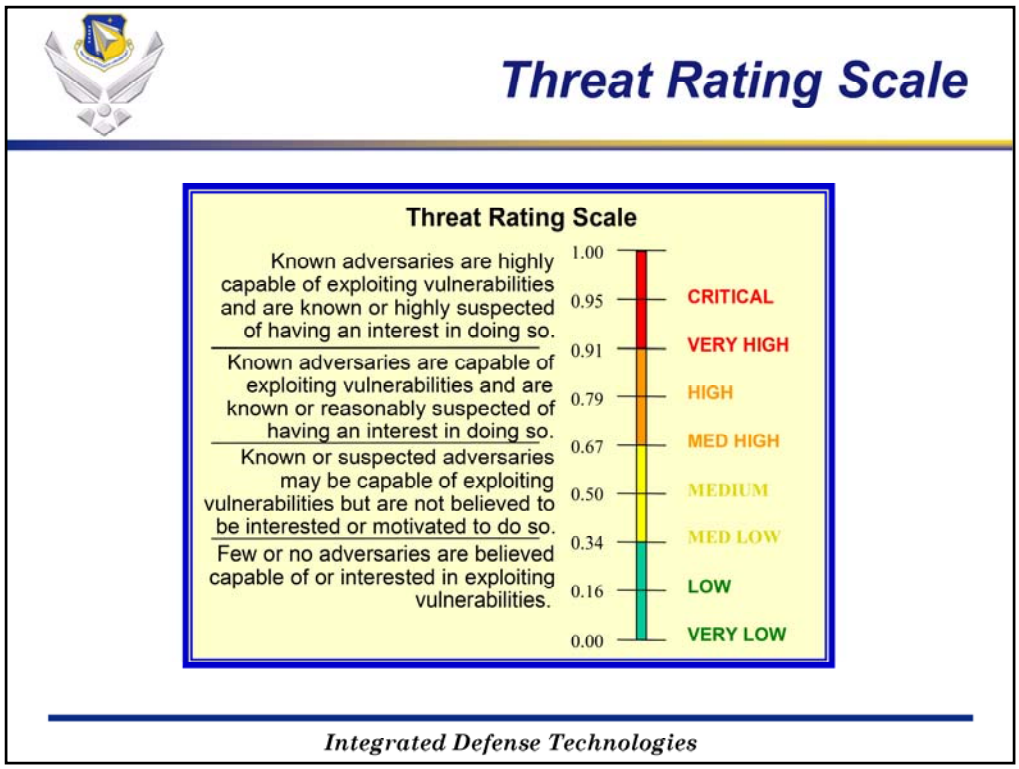
• We acknowledge the national threat from DIA with the Baseline International Terrorist rating (currently Significant in the US)

• We then identify, categorize and score the LOCAL actors/threats in the Area of Interest

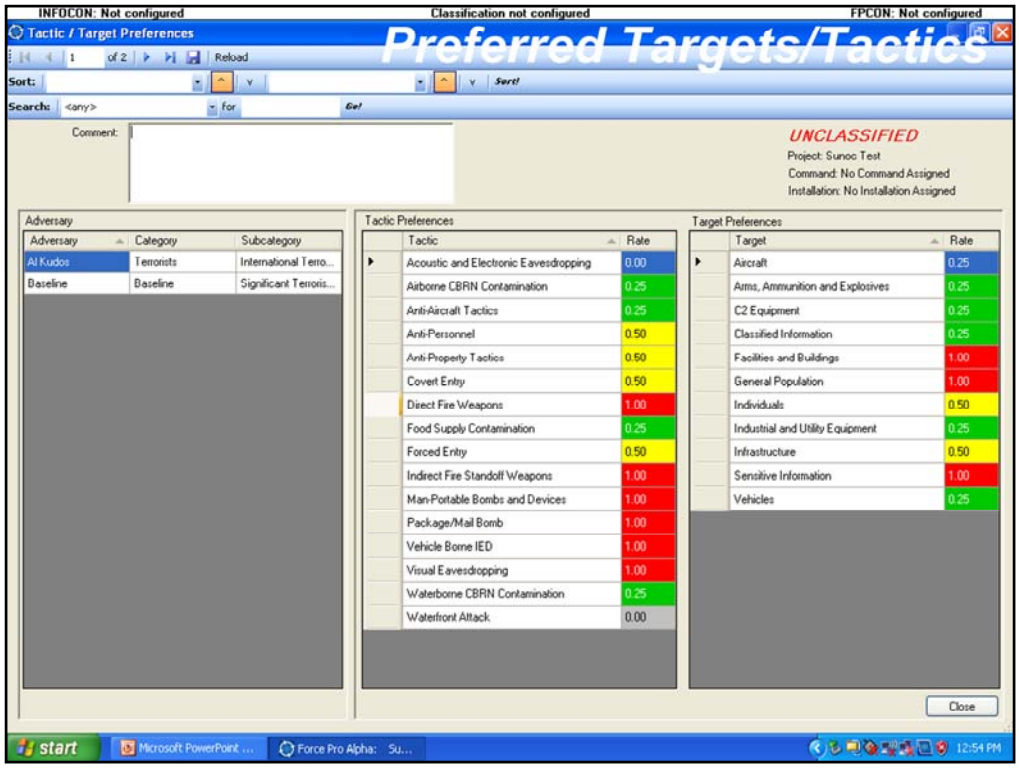
ForcePRO Tactics

Ballistic Tactics	Anti-Personnel Tactics
	Direct Fire Weapons
Contamination Tactics	Airborne CBRN Contamination
	Food Supply Contamination
	Waterborne CBRN Contamination
Eavesdropping Tactics	Acoustic and Electronic Eavesdropping
	Visual Eavesdropping
Explosives Tactics	Indirect Fire Standoff Weapons
	Man-Portable Bombs and Devices
	Package / Mail Bomb
	Vehicle-Borne IED
	Waterfront Attack
Property Tactics	Anti-Aircraft Tactics
	Anti-Property Tactics
	Covert Entry
	Forced Entry

- These 16 tactics are in the current version of ForcePRO
  - All require a malevolent adversary
  - Does not include natural disasters, insider threats, cyber



• Like the asset scale, this is the threat scale from 0 to 1.00



• Once you've identified the adversaries in the AI, you can tailor the default preferences for targets and tactics based on what you know about them

  • These are percentages, so 100 means they clearly prefer that target/tactic, 0 means they clearly do not, and numbers in between attempt to describe differing levels of interest and/or capability

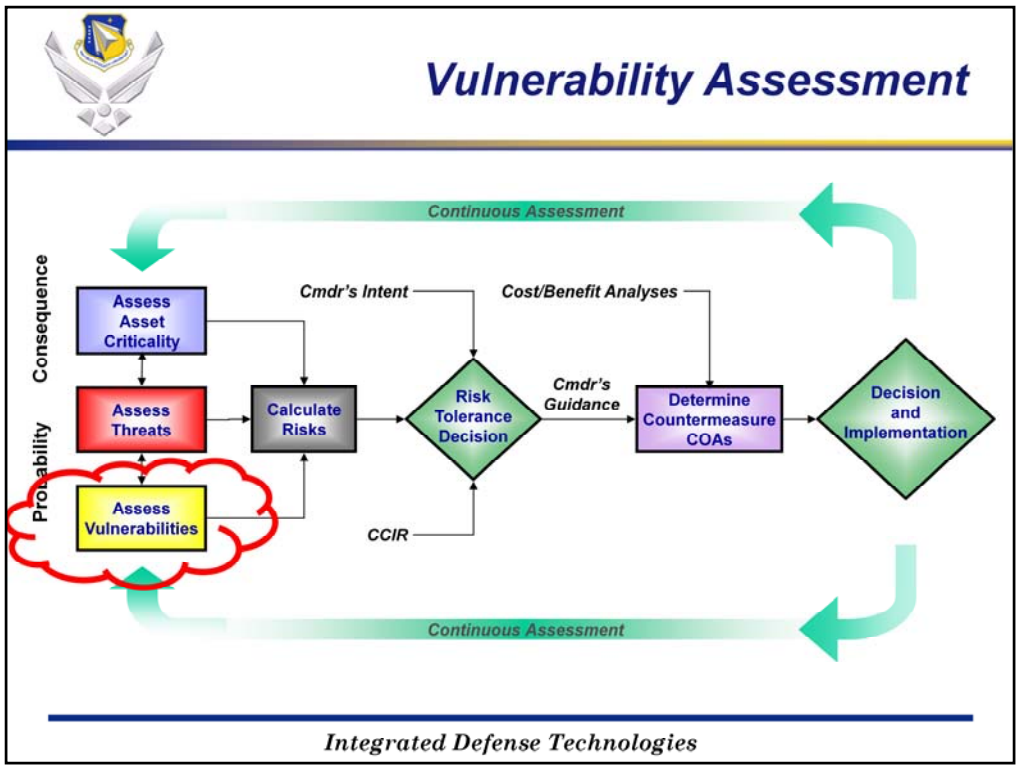
Consequence (Tactic Effectiveness) is handled in the Threat Rating

DEFAULT CONSEQUENCE EFFECTIVENESS MATRIX

100 = Destruction/Complete Loss
75 = Severe Damage
50 = Damage
25 = Cleanup/Nuisance Damage
0 = Ineffective/Inappropriate

			Targets											
			Equipment and Materials					Facilities and Buildings	Information		Infrastructure	People	
			Aircraft	Arms, Ammunition and Explosives	C2 Equipment	Industrial and Utility Equipment	Vehicles	Facilities and Buildings	Classified Information	Sensitive Information	Infrastructure	General Population	Individuals
Tactics	Ballistic	Anti-Personnel	0	0	0	0	0	50	0	0	0	75	100
		Direct Fire Weapons	75	50	50	50	50	75	0	0	25	100	100
	Contamination	Airborne CBRN Contamination	0	0	0	0	0	100	0	0	25	100	100
		Food Supply Contamination	0	0	0	0	0	100	0	0	0	100	100
		Waterborne CBRN Contamination	0	0	0	0	0	100	0	0	25	100	100
	Eavesdropping	Acoustic and Electronic Eavesdropping	0	0	75	0	0	50	100	100	0	50	50
		Visual Eavesdropping	50	50	0	0	0	50	100	100	0	50	50
	Explosives	Indirect Fire standoff Weapons	100	100	100	100	100	50	0	0	50	100	100
		Man-Portable Bombs and Devices	100	100	100	100	100	75	0	0	75	100	100
		Package/Mail Bomb	0	0	0	0	0	50	0	0	0	100	100
		Vehicle Borne IED	100	100	100	100	100	100	0	0	100	100	100
		Waterfront Attack	100	100	100	100	100	100	0	0	100	100	100
	Property	Anti-Aircraft Tactics	100	0	0	0	0	0	0	0	0	0	0
		Anti-Property Tactics	0	100	75	100	100	75	75	75	75	25	25
		Covert Entry	0	100	75	0	0	75	100	100	50	0	0
		Forced Entry	0	100	75	100	100	75	100	100	50	25	25

- Under the hood of ForcePRO (and not editable by the user) is the consequence effectiveness matrix
  - For the categories of target/tactic pairs, estimates how effective a tactic is against a target (e.g., vehicle bombs are more effective against buildings than letter bombs)
  - Also handles the inappropriate target/tactic pairs by assigning zeros (e.g., food contamination attack against vehicles)



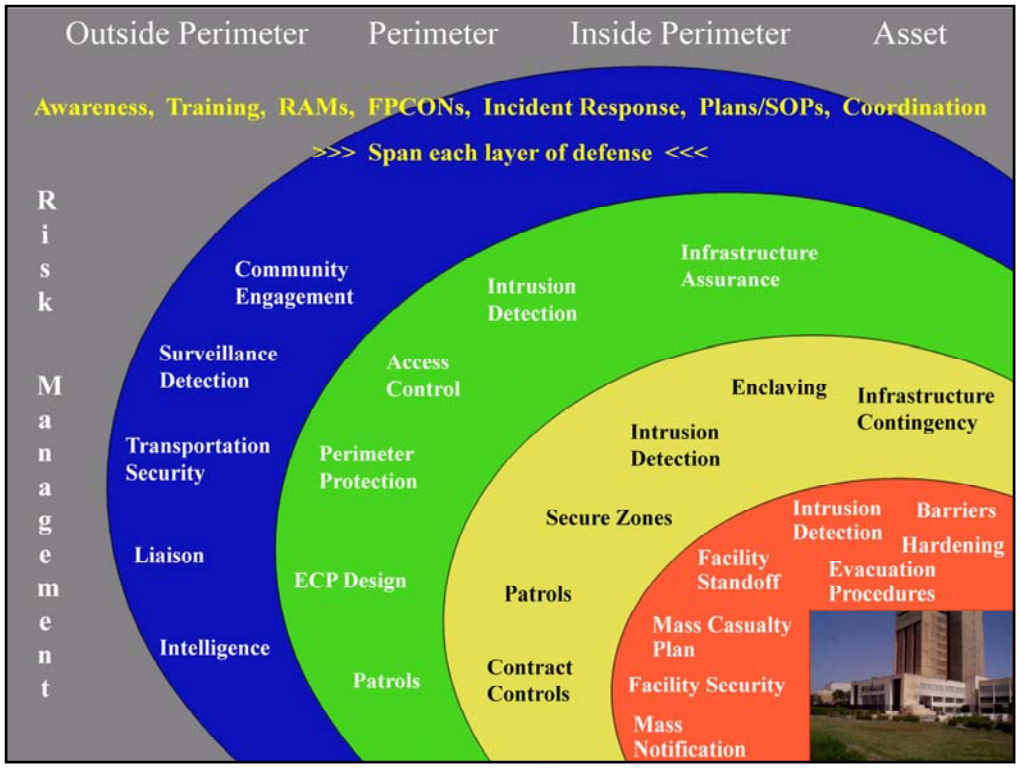
• The final risk factor is vulnerability … the "hole in the fence." Vulnerability may be the most subjective part of the Risk Analysis process. It is subjective because it's in the eye of the beholder on "how bad is bad."

- If the motivation behind the vulnerability assessment is find the "holes" that can get you hurt then you're fine. But if there is any bias behind the assessment the ratings are going to be skewed.
- For example, if the motivation is to have a great report and have an award winning program, then there is the potential the vulnerabilities will be understated. If the hidden agenda is to capture funds, then the vulnerabilities run the risk of being overstated.

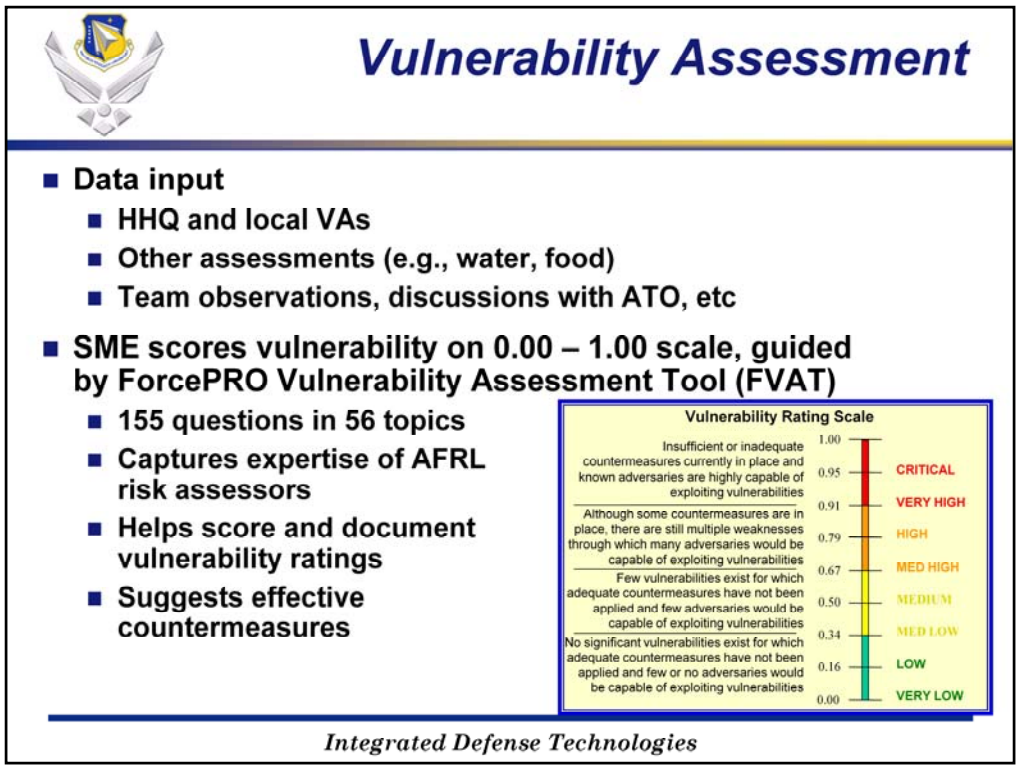
• In assessing vulnerability the basic question to answer is "What makes your assets easier to attack?"

• Evaluating the effectiveness of the countermeasure is often the most difficult part of the assessment … this is where bias comes into the forefront.

• Finally, where do you find the nuggets of info to help you make the right judgments regarding your countermeasures? Start with the SMEs on your base … a good rule of thumb is to "trust but verify."



- The slide depicts the concept of looking at vulnerability.
  - Usually we consider countermeasures in various installation *layers* as part of defense-in-depth. Rarely will a single countermeasure, or countermeasures located in a single layer, provide adequate security.
  - A typical layer breakdown might consider countermeasures outside the installation perimeter; at the perimeter; inside the perimeter; and at individual assets.



• The ForcePRO vulnerability assessment reviews the latest assessments, talks to local SMEs, and conducts its own investigations as required to understand the state of countermeasures at an installation

• Again, a 0 to 1.00 scale is used for vulnerability

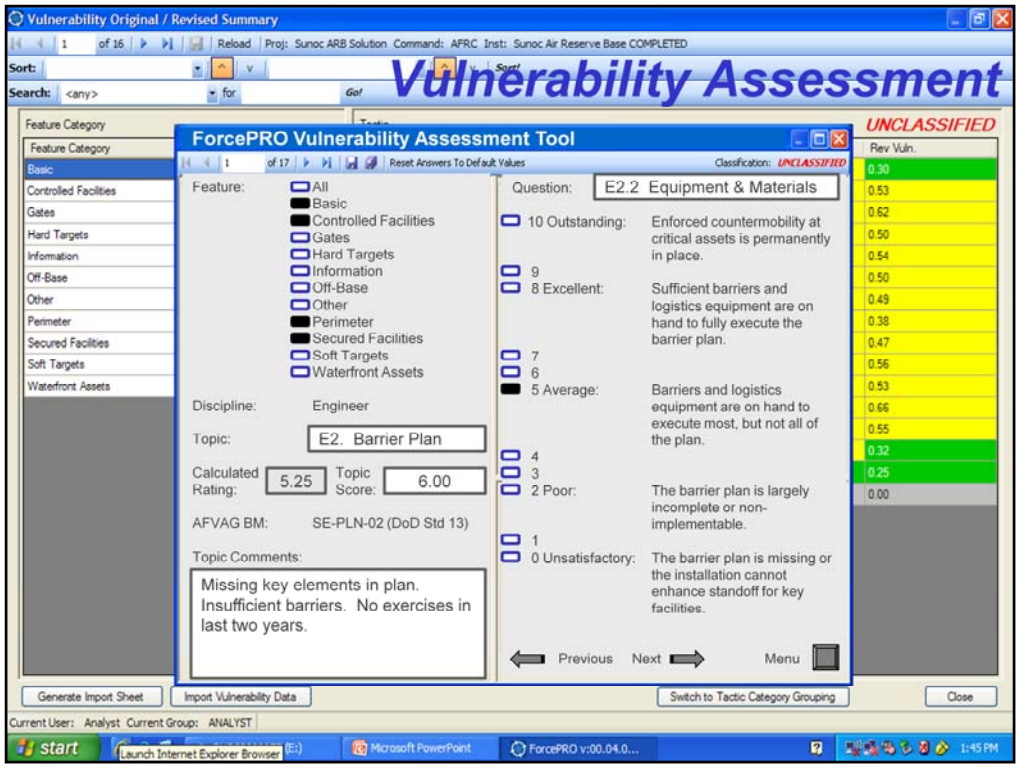
• The SMEs evaluate the vulnerabilities using FVAT (ForcePRO Vulnerability Assessment Tool)

  • Asks a series of questions (155 in 56 topics) that are rated from 0 to 10, with performance examples included

  • Five areas: Program, Intel, Security, Engineering, and Emergency Management

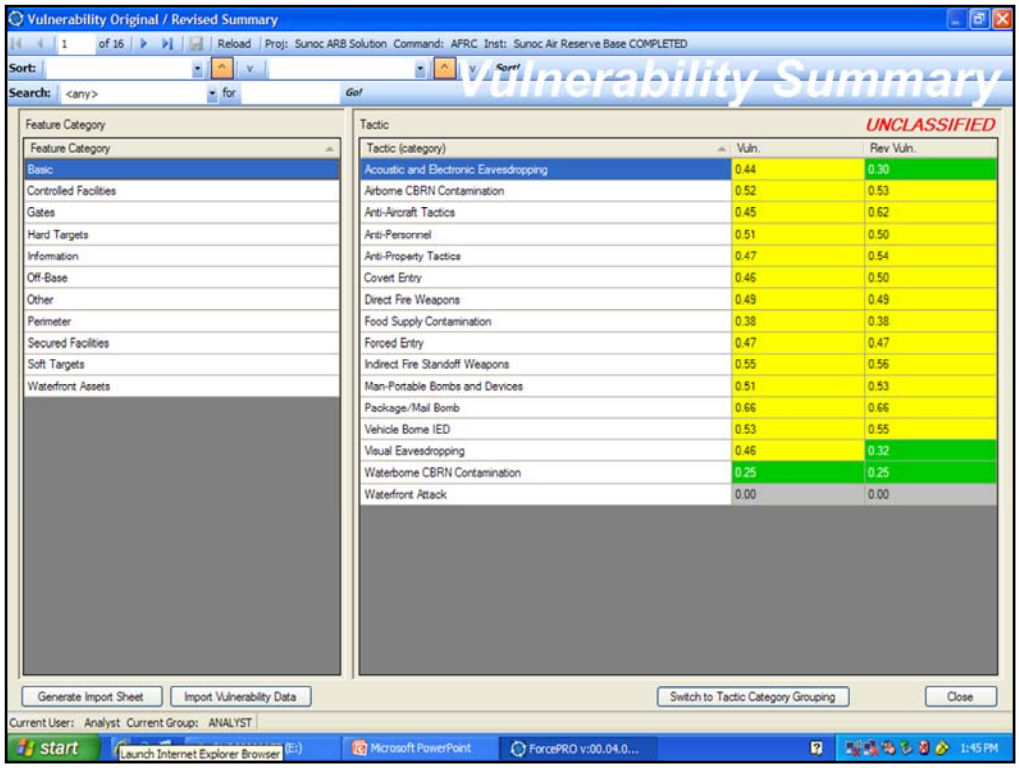
  • The FVAT tool helps score the vulnerabilities in a consistent fashion, and works with the ForcePRO tool

- This is a screen shot of the vulnerability tab
  - Organized by asset/tactic pairs
  - Often 1500 to 2000 or more asset/tactic pairs at this stage of a typical RA



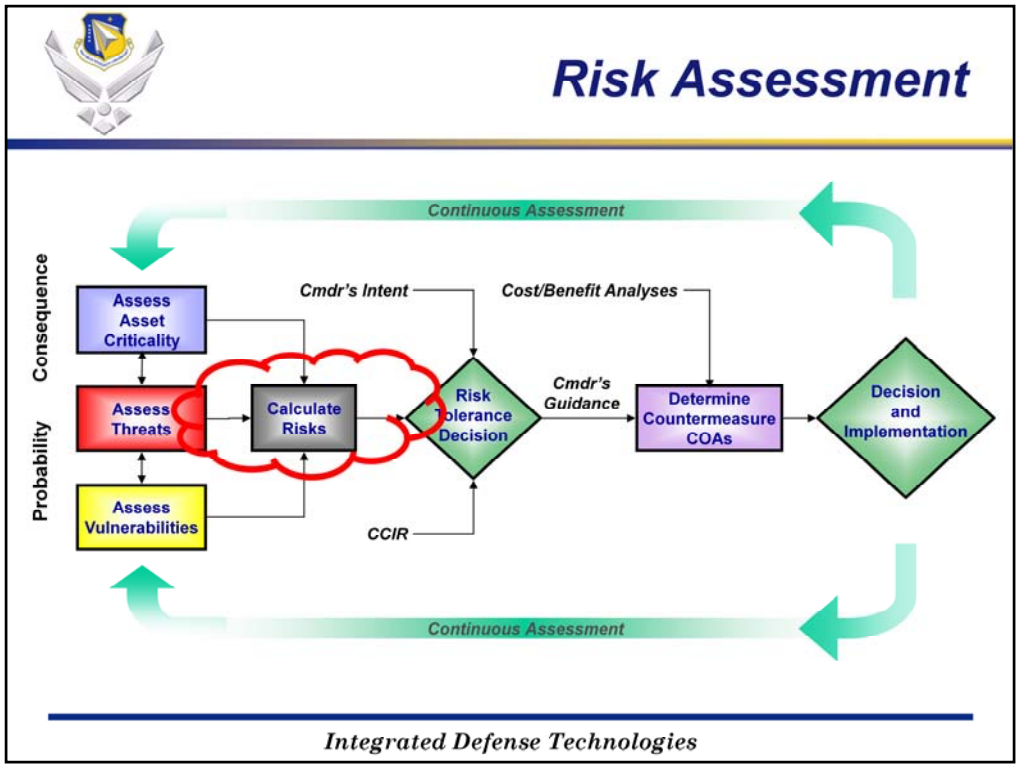
• FVAT uses a question format along with unsatisfactory to outstanding ratings to guide the analyst in developing a consistent vulnerability rating

  • The analyst is involved in every step, and can override the calculations (with justification) if the resulting rating does not reflect the true picture



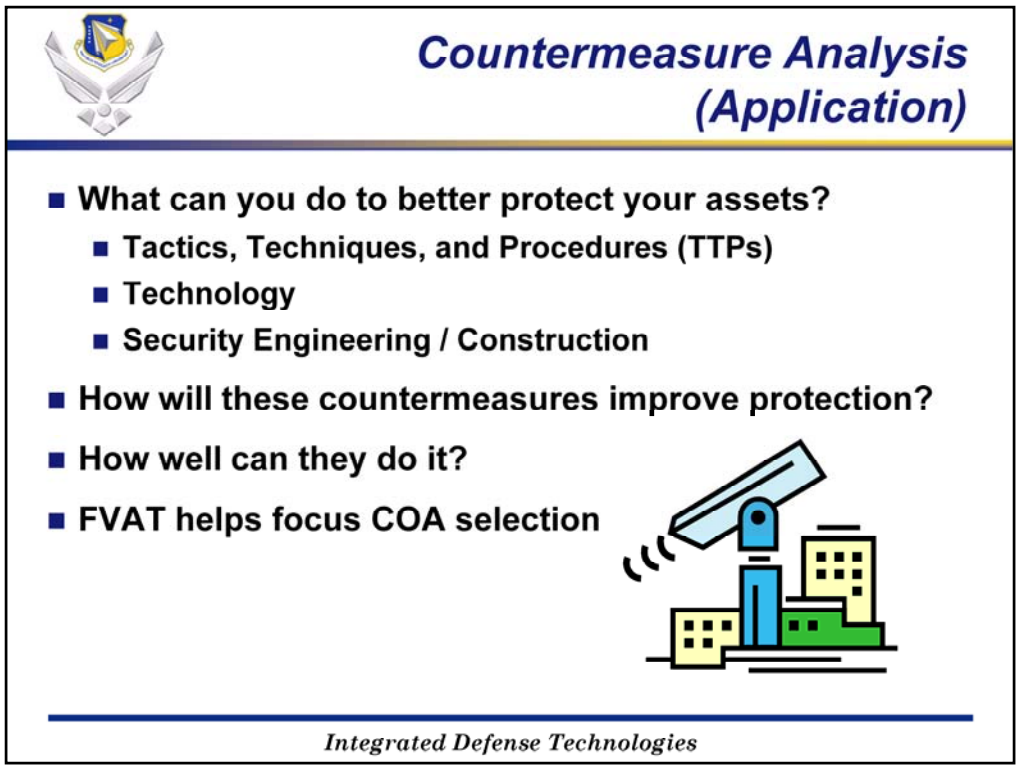
• ForcePRO is looking for vulnerability ratings for all 16 tactics in each feature category that applies to your installation (perimeter facilities, gates, hard/soft targets, off-base assets, etc)

  • You can enter vulnerability data in this screen, but much easier and quicker to use FVAT



• Now that we've assessed our criticality, threat and vulnerability, we multiply the values together to determine our risk score.

- The risk summary sheets shows the unwanted event (loss of asset due to tactic) plus scores for all three elements of risk and the risk score.
    - The analysis and ForcePRO allows you to have a logical, well structured discussion about risk.
- <click> At this stage, the commander may (hopefully) have enough information to make a risk tolerance decision to accept the risk, or to direct mitigation COAs to reduce it.
    - After you have the commander's risk decision it's time to move to countermeasure COA development.

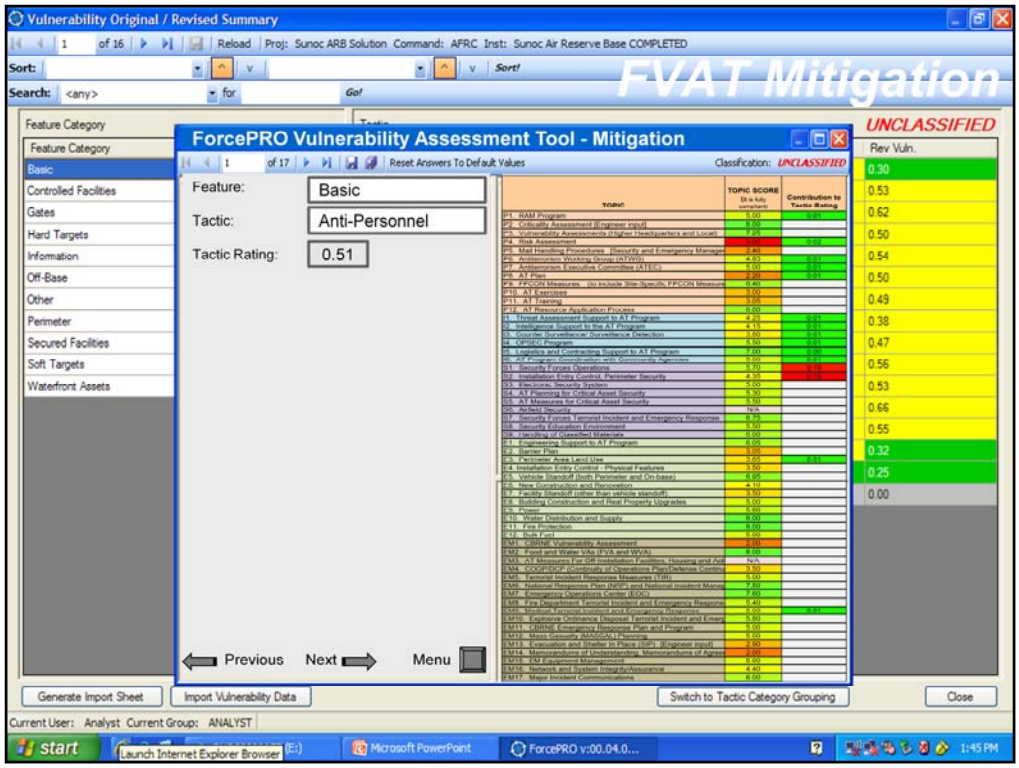


• In developing COAs keep in mind you have to work on developing COAs that are feasible. "Shutting the base down" for security operations is pretty much out, so our challenge is to develop an effective defense program, with the resources we have on hand, suitable for the risk we face, and offers the rest of the installation the freedom of movement to accomplish the installation missions.

- We can develop effective TTPs.
- We can invest in the right technology, the right way.
- We can use security engineering in construction projects to harden our perimeter and key assets.

• For any countermeasure we develop, we need to be able to provide a logical answer to "How will these countermeasures improve protection and how well?"

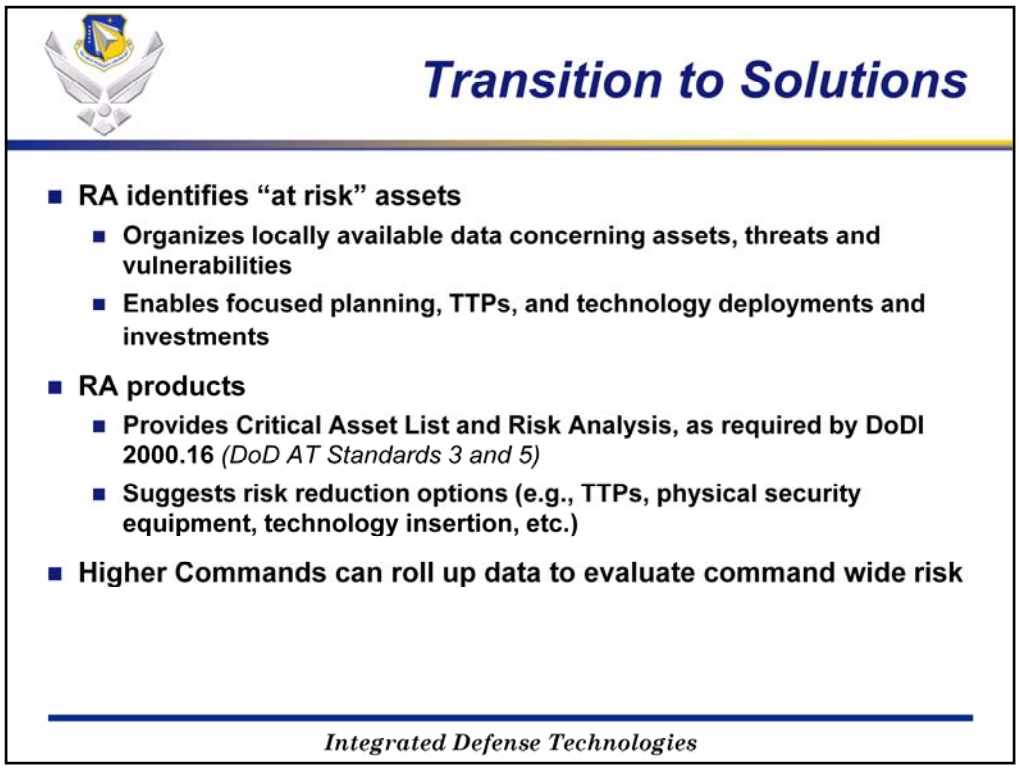
- The FVAT can help with COA selection by evaluating which countermeasure(s) are most effective in mitigating the unwanted event(s)



• The FVAT has a tool built in to help identify the most advantageous areas to improve

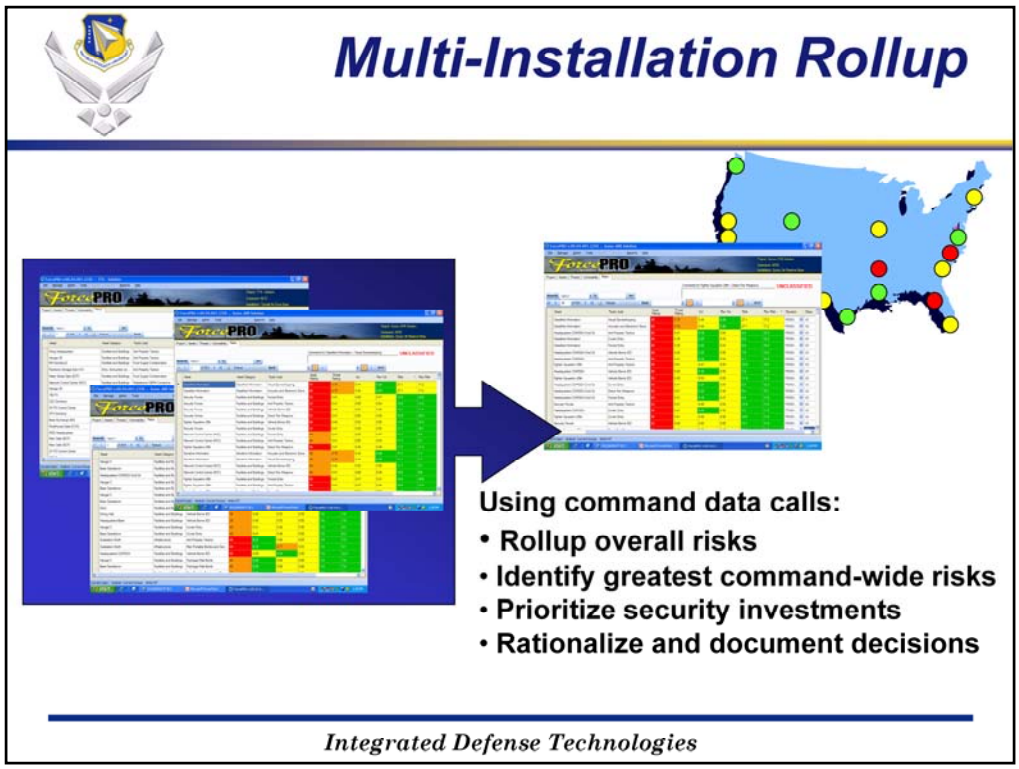
• Using FVAT, the RA team can estimate the reduction in risk if various COAs are implemented, providing the benefit part of a cost-benefit analysis

• The revised vulnerabilities are imported into ForcePRO, and revised risks calculated. The commander can now make implementation decisions regarding which COA he/she wants to pursue.



• A key element of the process and ForcePRO is that the methodology aids decisions. The RA in and of itself is meaningless without action and improvement

• Another tangible result of the RA are specific products (Criticality List, Risk Analysis) required by DoDI 2000.16



• Since the analysis was conducted using a standardized process, higher headquarters can use data calls to compare risks across their command and make prudent, supported decisions

ForcePRO and the risk-based decision making process we've described are being fielded for Air Force Security Forces as we speak. AFRL is currently conducting "train the trainer" courses for each Major Command, and will assist as the project is implemented Air Force wide.

The current version is an Oracle-based database tool that resides on stand-alone computers. We are also beginning efforts to develop a secure, network-based tool. This future ForcePRO will better integrate with existing databases to track implementation (Core Vulnerability Assessment and Management Program or CVAMP), and will also hyperlink to databases to aid in developing effective countermeasures.

Thank you for your attention. Are there any questions?